Hart L. Robinovitch (AZ #020910)
hart.robinovitch@zimmreed.com
ZIMMERMAN REED LLP
14648 North Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400

Brian C. Gudmundson (*pro hac vice forthcoming*)
brian.gudmundson@zimmreed.com
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400/Facsimile: (612) 341-0844

Kim D. Stephens, P.S. (*pro hac vice forthcoming*)
Cecily C. Jordan (*pro hac vice forthcoming*)
kstephens@tousley.com
cjordan@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992

Counsel for Plaintiff and the Proposed Class
**Pro Hac Vice Forthcoming*

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Karen Foti Williams, individually and on behalf of all others similarly situated, Plaintiff, v. Medical Management Resource Group, LLC d/b/a American Vision Partners, Defendant.	NO. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Karen Foti Williams ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Defendant Medical Management Resource Group, LLC d/b/a American Vision Partners ("Defendant" or "MMRG"). Plaintiff brings this action by and through her attorneys, and alleges, based upon personal knowledge as to her own actions, and based upon her information and belief and reasonable investigation by her counsel as to all other matters, as follows.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach on MMRG's network that resulted in unauthorized access to highly-sensitive patient data belonging to Plaintiff and nearly 2,400,000 Class Members.[1]

2. MMRG is an Arizona-based company providing a variety of administrative services to ophthalmology practices in Arizona and throughout the country.[2] MMRG markets itself as "one of the largest and fastest-growing eye care practice management organizations in the nation[.]"[3]

3. As part of its operations, MMRG collects, maintains, and stores highly sensitive personal and medical information belonging to patients, including, but not limited to: first and last names, dates of birth, Social Security numbers, and other demographic and contact information (collectively, "personally identifying information" or "PII"), health insurance information, information concerning patients' medical history, clinical records of mental or physical conditions, medical diagnosis and treatment, and other medical

[1] *See* U.S. Department of Health and Human Services, Currently Under Investigation, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb. 27, 2024); *see also MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

[2] American Vision Partners, *About – Our Story*, https://americanvisionpartners.com/about/our-story/ (last visited Feb. 28, 2024).

[3] American Vision Partners, *About – Press*, https://americanvisionpartners.com/about/press/ (last visited Feb. 28, 2024).

information from medical and billing records (collectively, "protected health information" or "PHI") (PII and PHI collectively are "Private Information").

4. On information and belief, former and current patients of MMRG's healthcare clients are required to entrust MMRG with sensitive, non-public Private Information, without which MMRG could not conduct its regular business activities, in order to obtain medical services.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, MMRG assumed legal and equitable duties to protect and safeguard that information from unauthorized access and intrusion.

6. MMRG claims it "takes the security of patients' data seriously[.]"[4] Despite these outward assurances, MMRG failed to adequately safeguard Plaintiff's and Class Members' highly-sensitive Private Information, which it collected, stored, and maintained.

7. According to MMRG, the Private Information compromised in the Data Breach includes: patient names, contact information, dates of birth, Social Security numbers, medical information such as services received, clinical records, and medications, and health insurance information.[5]

8. On information and belief, the cybercriminals accessed and stole Private Information belonging to the Plaintiff and Class Members as a direct and proximate result of MMRG's failure to adequately safeguard Plaintiff's and Class Members' highly sensitive Private Information.

9. MMRG owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information.

---

[4] *See MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

[5] *See* Data Breach Notice, **Exhibit A**; *see also* Steve Adler, *Medical Management Resource Group (American Vision Partners) Breach Affects 2.35M Patients*, The HIPAA Journal (Feb. 21, 2024), https://www.hipaajournal.com/mmrgamerican-vision-partners-breach-2-35m-patients/; *MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

Yet, MMRG maintained and shared the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on computer systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to MMRG, and thus MMRG was on notice that failing to take steps necessary to properly safeguard Plaintiff's and Class Members' Private Information from those risks would leave the Private Information in a vulnerable condition.

10. Plaintiff's and Class Members' Private Information was compromised due to MMRG's negligent and/or careless acts and omissions and MMRG's failure to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including: opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions, using Class Members' Private Information to obtain government benefits, and filing fraudulent tax returns using Class Members' Private Information.

12. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm, heightened here by the loss of Social Security numbers, a class of Private Information which is particularly valuable to identity thieves. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

13. This risk is even more pronounced given the extended amount of time that lapsed between when the Data Breach occurred, when MMRG reportedly determined Plaintiff's and Class Members' Private Information was compromised, and when MMRG actually notified Plaintiff and Class Members about the Data Breach.

14. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of

all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

15. As a result of MMRG's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class Members suffered injuries including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in MMRG's possession and is subject to further unauthorized disclosures so long as MMRG fails to undertake appropriate and adequate measures to protect their Private Information.

16. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of MMRG's failure to reasonably safeguard Plaintiff's and Class Members' Private Information; its failure to reasonably provide timely notification that Plaintiff's and Class Members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class Members concerning the status, safety, and protection of their Private Information.

17. Plaintiff brings this action against MMRG, seeking redress for MMRG's unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract;

(iii) unjust enrichment; (iv) bailment; and (v) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to MMRG's data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by MMRG.

PARTIES

18. Plaintiff Karen Foti Williams is a resident and citizen of the State of Arizona, residing in Maricopa County. Plaintiff is a former patient of Southwestern Eye Center, which is an MMRG client, partner and/or affiliate. Plaintiff Williams received a letter from MMRG dated February 15, 2024, notifying her that her Private Information was exposed in the Data Breach.

19. Defendant Medical Management Resource Group, LLC d/b/a American Vision Partners is a limited liability company formed under the state laws of Arizona, with its principal place of business located at 2120 E. Rio Salado Parkway, Suite 220, Tempe, Arizona 85281.

JURISDICTION AND VENUE

20. This Court has original jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

21. This Court has general personal jurisdiction over Defendant because Defendant operates in and directs commerce at this District and maintains its principal place of business in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)-(d) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Defendant's Business

23. Defendant MMRG is an Arizona-based company that provides a variety of administrative services to ophthalmology practices in Arizona and throughout the country.[6]

24. On information and belief, in the ordinary course of its business of providing services to its healthcare clients, MMRG maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number or taxpayer identification number;
- Financial and/or payment information;
- Health billing information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health information;
- Other information that MMRG may deem necessary to provide services and care.

25. Additionally, MMRG may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

26. Because of the highly sensitive and personal nature of the information MMRG acquires and stores with respect to consumers and other individuals, MMRG, upon

[6] American Vision Partners, *About – Our Story*, https://americanvisionpartners.com/about/our-story/ (last visited Feb. 28, 2024).

information and belief, promises to, among other things: keep Private Information private; comply with financial industry standards related to data security and Private Information, including FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from MMRG and provide adequate notice to individuals if their Private Information is disclosed without authorization.

27. As a HIPAA covered business entity, MMRG is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the Data Breach complained of herein.

28. However, MMRG did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly three months to publicly disclose the Data Breach to consumers.[7]

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, MMRG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

30. Yet, contrary to MMRG's representations, MMRG failed to implement adequate data security measures, as evidenced by its admission of the Data Breach, which affected nearly 2,400,000 individuals.

31. Current and former patients of MMRG's healthcare clients, such as Plaintiff and Class Members, made their Private Information available to MMRG with the reasonable expectation that any entity with access to this information would keep that

[7] *See MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

sensitive and personal information confidential and secure from illegal and unauthorized access. And, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

32. This expectation was objectively reasonable and based on an obligation imposed on MMRG by statute, regulations, industry standards, and standards of general due care.

33. Unfortunately for Plaintiff and Class Members, MMRG failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiff and Class Members from having their Private Information accessed and stolen during the Data Breach.

B. Defendant MMRG Is a Covered Entity Subject to HIPAA

34. Defendant MMRG is a HIPAA covered entity, providing administrative services to millions of patients annually via its healthcare and medical practice clients. As a regular and necessary part of its business, MMRG collects the highly-sensitive Private Information of patients. As a covered entity, MMRG is required under federal and state law to maintain the strictest confidentiality of the Private Information that it acquires, receives, collects, and stores. MMRG is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

35. Due to the nature of MMRG's business, which includes providing a range of services to patients and healthcare clients, including obtaining, storing, and maintaining electronic health records, MMRG would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

36. Plaintiff and Class Members are or were patients, or are the executors or surviving spouses of patients, whose Private Information was maintained by MMRG and directly or indirectly entrusted MMRG with their Private Information.

37. Plaintiff and Class Members relied on MMRG to implement and follow adequate data security policies and protocols, to keep their Private Information confidential

and securely maintained, to use such Private Information solely for business and healthcare purposes, and to prevent unauthorized disclosures of Private Information. Plaintiff and Class Members reasonably expected that MMRG would safeguard their highly sensitive information and keep that Private Information confidential.

38. As described throughout this Complaint, MMRG did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly-sensitive Private Information that it maintained. Consequently, cybercriminals circumvented MMRG's security measures, resulting in a significant data breach.

C. The Data Breach and Notice Letter

39. According to the notice letter MMRG sent to Plaintiff and Class Members (the "Data Breach Notice"),[8] MMRG was subject to a cybersecurity attack that allowed unauthorized parties to access and compromise Plaintiff's and Class Members' Private Information.

40. On November 14, 2023, MMRG "detected unauthorized activity on certain parts of [its] network."[9] In response, MMRG "launched an investigation with the assistance of leading third-party cybersecurity firms[.]"[10]

41. On or around December 6, 2023, MMRG determined that an "unauthorized party obtained personal information associated with patients of [MMRG's clients]."[11]

42. According to MMRG, the Private Information compromised in the Data Breach includes: patient names, contact information, dates of birth, Social Security numbers, medical information such as services received, clinical records, and medications,

[8] Data Breach Notice, **Exhibit A**; *see also MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

[9] *See id.*

[10] *Id.*

[11] *Id.*

and health insurance information.[12]

43. On February 6, 2024, MMRG filed a notice of data breach with the U.S. Department of Health and Human Services Office for Civil Rights, confirming the Private Information of nearly 2,400,000 individuals was accessed and stolen in the Data Breach.[13]

44. MMRG waited nearly three months from the date it learned of the Data Breach, and the highly sensitive nature of the Private Information impacted, to publicly disclose the Data Breach and notify affected individuals.

45. In the aftermath of the Data Breach, MMRG has not indicated any measures it has taken to mitigate the harm beyond "continu[ing] to take preventative actions to further safeguard its systems."[14] There is no indication whether these measures are adequate to protect Plaintiff's and Class Members' Private Information going forward.

46. According to MMRG, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the Data Breach.

47. The accessed data contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

48. As a HIPAA covered business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk which MMRG was aware of and knew it had a duty to guard against. It is well-known that healthcare providers and their business associates, like MMRG, which collect and store the confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the

---

[12] *See id.*; *see also* Steve Adler, *Medical Management Resource Group (American Vision Partners) Breach Affects 2.35M Patients*, The HIPAA Journal (Feb. 21, 2024), https://www.hipaajournal.com/mmrgamerican-vision-partners-breach-2-35m-patients/.

[13] *See* U.S. Department of Health and Human Services, Currently Under Investigation, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb. 27, 2024).

[14] *See* Data Breach Notice, **Exhibit A**; *see also MMRG Notifies Patients of Cybersecurity Incident*, Business Wire (Feb. 6. 2024), https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident.

implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

49. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

50. MMRG had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

51. Plaintiff and Class Members entrusted MMRG (or their doctors and healthcare providers) with their Private Information with the reasonable expectation and mutual understanding that MMRG would comply with its obligations to keep such information confidential and secure from unauthorized access.

52. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, MMRG assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

53. Due to MMRG's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

D. Defendant MMRG's Failure to Protect Patient's Private Information

54. MMRG collects and maintains vast quantities of Private Information belonging to patients, including Plaintiff and Class Members, as part of its normal business operations. The Data Breach occurred as a direct, proximate, and foreseeable result of multiple failings on the part of MMRG.

55. MMRG inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

56. MMRG failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class Members been aware that MMRG did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to MMRG (or their doctors and healthcare providers).

57. Plaintiff's and Class Members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. They face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

E. The Data Breach was a Foreseeable Risk of which Defendant MMRG was on Notice

58. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII and PHI, and Social Security numbers in particular, are an invaluable commodity and a frequent target of hackers.

59. As a HIPAA-covered entity handling medical patient data, MMRG's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

60. At all relevant times, MMRG knew or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, MMRG failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that MMRG should have anticipated and guarded against.

61. In light of recent high profile data breaches at other health care providers, MMRG knew or should have known that its electronic records and consumers' Private

Information would be targeted by cybercriminals and ransomware attack groups

62. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[15] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just eight shy of the record of 715 set in 2021, and still double that of the number of similar such compromises in 2017.[16]

63. Cyber criminals target institutions which collect and store PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were at least 905 health data breaches in 2021, impacting over 50 million patients. The report noted that "the volume and impact of breaches continue to be underreported overall, and underrepresented to the public[,]" stressing that "gaps in detection and reporting mean the true impact of incidents is likely even greater."[17]

64. The healthcare sector suffered at least 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[18]

---

[15] *2022 End of Year Data Breach Report*, Identity Theft Resource Center at 6 (Jan. 25, 2023), *available at* https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed Mar. 4, 2024).

[16] *2022 Healthcare Data Breach Report*, The HIPAA Journal (Jan. 24, 2023), *available at* https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed Mar. 4, 2024).

[17] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last visited Mar. 4, 2024).

[18] *See* Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY: CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

65. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant MMRG knew or should have known that its electronic records would be targeted by cybercriminals.

66. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII[.]" The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[19]

67. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[20] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[21] A study by Experian found that the "average total cost" of medical identity theft was "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22]

---

[19] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[20] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[21] *Id.*

[22] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

68. In fact, according to the cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyberattacks in 2020.[23]

69. Cyberattacks on medical systems have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

70. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into medical practices for their highly prized medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights (OCR)] – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[25]

71. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[26] In this case, Defendant MMRG stored the records of *millions* of patients.

72. Private Information, like that stolen from MMRG, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold

---

[23] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[24] *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[25] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

[26] *See id*.

on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[27]

73. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

74. MMRG was on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[28]

75. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[29]

76. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

77. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal

---

[27] *See id.*

[28] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[29] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[30]

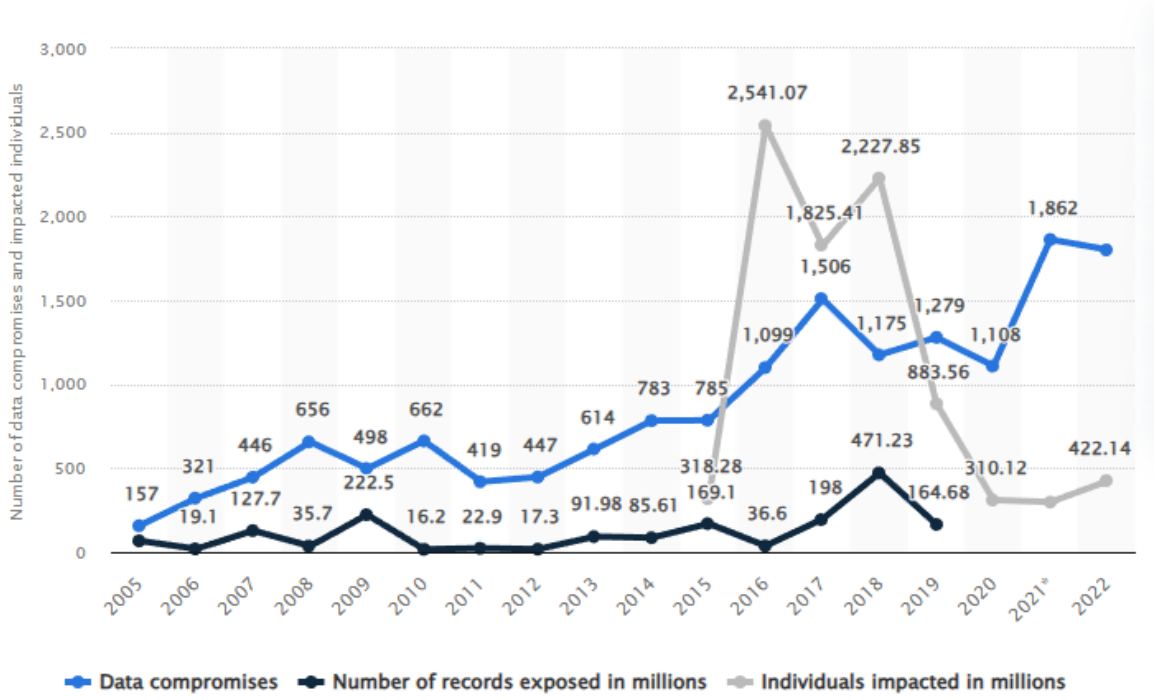
78. As a HIPAA covered entity, MMRG should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

79. Statista, a German entity that collects and markets data relating to data breach incidents and their consequences, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005; it reported 157 compromises in 2005, to a peak of 1,862 in 2021, to 2022's total of 1,802.[31] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[32]

[30] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

[31] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, *available at* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last accessed Mar. 4, 2024).

[32] *Id.*



80. This stolen Private Information is then routinely traded on dark web black markets as a simple commodity.[33]

81. Armed with just a name and Social Security number, criminals can fraudulently take out loans under a victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[34]

[33] Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (Sept. 28, 2021), *available at* https://cybernews.com/security/whats-your-identity-worth-on-dark-web/ (last accessed Mar. 4, 2024).

[34] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration at 1 (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 4, 2024).

82. The problems associated with a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing her or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[35]

83. The most sought after and expensive pieces of information on the dark web are stolen medical records, which command prices from $250 to $1,000 each.[36] Medical records are considered the most valuable because—unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed—medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[37] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[38] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[39] Victims of

---

[35] *Id.*

[36] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), *available at* https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last accessed Mar. 4, 2024).

[37] *Id.*

[38] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), *available at* https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed Mar. 4, 2024); *see also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), *available at* https://www.consumerreports.org/health/medical-identity-theft-a1699327549/ (last accessed Mar. 4, 2024).

[39] *Id.*

medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[40]

84. The wrongful use of compromised medical information is known as medical identity theft, and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[41] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[42]

85. Instances of medical identity theft have grown exponentially over the years, from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[43]

86. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like MMRG—which are charged with maintaining and securing patient PII and PHI—should know the importance of protecting that information from unauthorized disclosure. Indeed, MMRG knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[44]

87. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving

---

[40] *Id.*

[41] Medical Identity Theft, AARP (Feb. 15, 2019), *available at* https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last accessed Mar. 4, 2024).

[42] *Id.*

[43] *Id.*

[44] *See, e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, *available at* https://www.hipaajournal.com/healthcare-data-breach-statistics (last accessed Mar. 4, 2024).

inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like MMRG on notice of their obligation to safeguard customer and patient information.[45]

88. Given the nature of MMRG's Data Breach, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in their names.

89. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information, because credit card victims can cancel or close credit and debit card accounts.[46] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

90. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, MMRG failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by MMRG's failure to implement or maintain adequate data security measures for its current and former patients.

---

[45] *See, e.g.*, In the Matter of SKYMED INTERNATIONAL, INC., C-4732, 1923140 (F.T.C. Jan. 26, 2021).

[46] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), *available at* https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=3d3108f813f1 (last accessed Mar. 4, 2024); *see also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), *available at* https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/ (last accessed Mar. 4, 2024).

F. Defendant MMRG Had a Duty and Obligation to Protect Private Information

91. Defendant MMRG has an obligation to protect Plaintiff's and Class Members' Private Information. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and PHI. And third, MMRG imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class Members provided, and MMRG obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violations

92. HIPAA requires, among other things, that covered entities and their business associates implement and maintain policies, procedures, systems, and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI; protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI; regularly review access to data bases containing protected information; and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

93. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology[.]" 45 CFR § 164.402.

94. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires MMRG to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***." (emphasis added).

95. Upon information and belief, MMRG failed to implement and/or maintain procedures, systems, and safeguards to protect the PII and PHI belonging to Plaintiff and the Class from unauthorized access and disclosure.

96. Upon information and belief, MMRG's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information MMRG creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by MMRG's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

97. Upon information and belief, MMRG also failed to store the information it collected in a manner that rendered it "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

98. Because MMRG failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to

ensure MMRG's approach to information security is adequate and appropriate going forward. On information and belief, MMRG still maintains the PHI and other highly-sensitive PII of its clients' current and former patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

2. FTC Act Requirements and Violations

99. The Federal Trade Commission has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

100. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[47] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[48] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and

[47] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Mar. 4, 2024).

[48] *Id.*

have a response plan ready in the event of a breach.[49] MMRG clearly failed to do any of the foregoing, as evidenced by the Data Breach itself.

101. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. Additionally, the FTC Health Breach Notification Rule obligates companies that suffer a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

104. As evidenced by the Data Breach, MMRG failed to properly implement basic data security practices. MMRG's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

105. MMRG was fully aware of its obligation to protect the Private Information of its clients' current and former patients, including Plaintiff and Class Members, as MMRG is a sophisticated and technologically savvy healthcare group that relies extensively on technology systems and networks to maintain its practice, including storing patients' Private Information, in order to operate its business.

[49] *Id.*

106. MMRG had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information of Plaintiff and the Class from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between MMRG and Plaintiff and Class Members. MMRG alone had the exclusive ability to implement adequate security measures to its cybersecurity network to secure and protect Plaintiff's and Class Members' Private Information.

3. Industry Standards and Noncompliance

107. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

108. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like MMRG, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data.

109. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

110. On information and belief, Defendant MMRG failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

111. These foregoing frameworks are existing and applicable industry standards

in the healthcare industry, and MMRG failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at Risk

112. Cyberattacks and data breaches at healthcare service providers and their business associates, like MMRG, are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

113. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[50]

114. Researchers have further found that for medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes.[51]

115. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[52]

116. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about

---

[50] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[51] *See* Sung J. Choi, et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[52] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

117. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[53]

118. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

119. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

120. Moreover, theft of Private Information is also gravely serious because

[53] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Mar. 4, 2024).

Private Information is an extremely valuable property right.[54]

121. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

122. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

123. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> GAO Report at 29.

124. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

125. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

126. Private Information can sell for as much as $363 per record according to the

[54] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

Infosec Institute.[55] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

127. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[56] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[57] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

128. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

129. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[58]

130. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social

---

[55] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[56] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

[57] *Id.*

[58] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

Security Numbers are worth more than 10x on the black market."[59]

131. Medical information is especially valuable to identity thieves.

132. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[60]

133. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

134. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

135. For this reason, Defendant MMRG knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant MMRG was on notice of the substantial and foreseeable risk of harm from a data breach, yet MMRG failed to properly prepare for that risk.

H. Defendant MMRG's Data Breach

136. Defendant MMRG breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. MMRG's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

---

[59] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[60] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 4, 2024).

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

137. Defendant MMRG negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

138. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with MMRG.

I. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

139. Like any data breach, the Data Breach in this case presents major problems for all affected.[61]

140. The FTC warns the public to pay particular attention to how they keep PII, including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[62]

[61] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), *available at* https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last accessed Mar.4 2024).

[62] *Warning Signs of Identity Theft*, Federal Trade Comm'n, *available at* https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed Mar. 4, 2024).

141. The ramifications of MMRG's failure to properly secure Plaintiff's and Class Members' Private Information are severe. Identity theft occurs when someone uses another person's financial, medical, or personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

142. PII has a long shelf-life because it can be used in more ways than one, and it typically takes time for an information breach to be detected.

143. Plaintiff and Class Members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI and then risk prosecution by listing it for sale on the dark web if the PII and PHI was not valuable to malicious actors.

144. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

145. Malicious actors can use Private Information to gain access to Class Members' digital lives, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

146. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

147. Malicious actors can use Class Members' Private Information to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

148. As established above, the Private Information accessed in the Data Breach is also very valuable to MMRG. MMRG collects, retains, and uses this information to increase profits. MMRG's clients value the privacy of this information and expect MMRG to allocate enough resources to ensure it is adequately protected. Customers would not have done business with MMRG, provided their PII and PHI, and/or paid the same prices for MMRG's services had they known MMRG did not implement reasonable security measures to protect their PII and PHI. Patients expect that the payments they make to the medical providers incorporate the costs to implement reasonable security measures to protect their Private Information.

149. The Private Information accessed in the Data Breach is also very valuable to Plaintiff and Class Members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class Members' PII has been compromised and lost significant value.

150. Plaintiff and Class Members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often

significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiffs and Class Members will therefore need to continuously monitor their accounts for years to ensure their Private Information obtained in the Data Breach is not used to harm them.

151. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

152. Accordingly, MMRG's wrongful actions and inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

153. According to a recent study published in the scholarly journal "Preventive Medicine Reports," public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[63] The same study also found that identity theft is a deeply traumatic event for victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[64]

154. There is also a high likelihood that significant identity fraud and identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals may be exploited in the future; there is a concrete risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

155. Data breaches have proven to be costly for affected organizations as well, with the average cost to resolve a data breach in 2023 at $4.45 million.[65] The average cost

---

[63] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and Protective Factors of Identity Theft Victimization in the United States*, Preventive Medicine Reports, Volume 17 (March 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub (last accessed Mar. 4, 2024).

[64] *Id.*

[65] *Cost of a Data Breach Report 2023*, IBM Security, *available at* https://www.ibm.com/reports/data-

to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[66]

156. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years, and this explosive growth far outstrips the increase in incidence of traditional identity theft. Medical identity theft is especially harmful for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[67]

157. Here, due to the Breach, Plaintiff and Class Members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and health insurance information as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, monitoring claims made against their health insurance, lost productivity and opportunities, time taken from the enjoyment of

---

breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds (last accessed Mar. 4, 2).

[66] *Id.*

[67] *Id.*

one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; and

e. The loss of Plaintiff's and Class Members' privacy.

158. Plaintiff and Class Members have suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will continue for years and years. The unauthorized access of Plaintiff's and Class Members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely.

159. As a direct and proximate result of MMRG's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class Members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

160. In addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose Private Information was accessed and compromised in the Data Breach, Plaintiff retains an interest in ensuring there are no future breaches. On information and belief, MMRG is still in possession, custody, and/or control of Plaintiff's and the Class Members' Private Information.

J. Plaintiff's Experience

161. Plaintiff Karen Foti Williams is a former patient of Southwestern Eye Center, which is a client, partner, and/or affiliate of MMRG.

162. According to the Data Breach Notice letter Plaintiff received, her Private Information was impacted in the Data Breach.

163. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving medical services that required her PII and PHI. Upon information and belief, Defendant MMRG received and maintains the information Plaintiff was required to provide to her doctors or medical professionals.

164. Plaintiff is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

165. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

166. Plaintiff was forced to date to spend approximately one hour attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

167. Plaintiff suffered actual injury and damages from having her Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that MMRG obtained from Plaintiff and/or Plaintiff's doctors and medical professionals; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) failure to receive the benefit of her bargain; and (g) nominal and statutory damages.

168. Plaintiff has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her Social Security number, medical records, and prescriptions.

169. As a result of the Data Breach, Plaintiff anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

170. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in MMRG's possession, is protected and safeguarded from future breaches.

CLASS REPRESENTATION ALLEGATIONS

171. Plaintiff brings this action against Defendant MMRG individually and on behalf of all other persons similarly situated (the "Class").

172. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

173. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

174. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

175. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The U.S. Department of Health and Human Services investigation reports that nearly 2,400,000 individuals were impacted by Defendant's Data Breach.[68]

176. Commonality. There are questions of law and fact common to the Class,

[68] U.S. Department of Health and Human Services, Currently Under Investigation, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb. 27, 2024).

which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

177. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

178. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

179. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

180. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

181. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

182. Likewise, particular issues are appropriate for certification because such

claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

183. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

COUNT I
Negligence

(*On Behalf of Plaintiff and the Class*)

184. Plaintiff re-alleges and incorporates by reference the above paragraphs numbered 1 to 170 as if fully set forth herein.

185. By collecting and storing the Private Information of Plaintiff and Class Members, in its computer systems and networks, and sharing it and using it for commercial

gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

186. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

187. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

188. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

189. Defendant MMRG's duty to use reasonable security measures under HIPAA required MMRG to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

190. In addition, Defendant MMRG had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and

enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

191. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

192. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;
b. Failing to adequately monitor the security of its networks and systems;
c. Failing to ensure that its email systems had plans in place to maintain reasonable data security safeguards;
d. Failing to have in place mitigation policies and procedures;
e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;
f. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and
g. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

193. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendant's possession.

194. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the

healthcare industry.

195. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

196. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

197. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

199. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

200. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract

(On behalf of Plaintiff and the Class)

201. Plaintiff re-alleges and incorporates by reference the above paragraphs numbered 1 to 170 as if fully set forth herein.

202. Defendant acquired and maintained the Private Information of Plaintiff and the Class that they received either directly or from their healthcare providers.

203. When Plaintiff and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, revenue service providers, and other service providers, including MMRG.

204. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

205. Plaintiff and the Class were required to deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

206. Defendant MMRG solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant, or, alternatively, provided their information to doctors or other healthcare professionals, who then provided it to Defendant.

207. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members and/or

their doctors and other healthcare professionals.

208. In accepting such information and payment for services, Defendant entered into implied contracts with Plaintiff and Class Members whereby Defendant became obligated to reasonably safeguard Plaintiff's and Class Members' Private Information.

209. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendant and healthcare providers.

210. In delivering, directly or indirectly, their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

211. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

212. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

213. Plaintiff and Class Members (or their doctors and healthcare providers) would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

214. Had Defendant disclosed to Plaintiff and Class Members (or their doctors and healthcare providers) that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to Defendant.

215. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members (or their doctors and healthcare providers).

216. Plaintiff and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with Defendant.

217. Defendant breached the implied contracts with Plaintiff and Class Members (or their doctors and healthcare providers) by failing to take reasonable measures to safeguard their Private Information as described herein.

218. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment

(On Behalf of Plaintiff and the Class)

219. Plaintiff re-alleges and incorporates by reference the above paragraphs numbered 1 to 170 as if fully set forth herein.

220. This count is pleaded in the alternative to breach of contract.

221. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from money it makes based upon protecting Plaintiff's and Class Members' Private Information.

222. There is a direct nexus between money paid to Defendant and the requirement that Defendant keeps Plaintiff's and Class Members' Private Information confidential and protected.

223. Plaintiff and Class Members paid Defendant and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendant.

224. As such, a portion of the payments made by or on behalf of Plaintiff and

Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

225. Protecting the Private Information of Plaintiff and Class Members is integral to Defendant's businesses. Without their data, Defendant MMRG would be unable to provide the services to patients, hospitals and healthcare providers comprising MMRG's core business.

226. Plaintiff's and Class Members' data and Private Information has monetary value.

227. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from entities that contracted with Defendant, and from which Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by supplying Private Information, which has value, from which value Defendant derives its business value, and which should have been protected with adequate data security.

228. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

229. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failures to provide the requisite security.

230. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because

Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

231. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

232. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant (or to their physician to provide to Defendant).

233. Plaintiff and Class Members have no adequate remedy at law.

234. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

235. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

236. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
Bailment

(*On Behalf of Plaintiff and the Class*)

237. Plaintiff re-alleges and incorporates by reference the above paragraphs numbered 1 to 170 as if fully set forth herein.

238. Plaintiff and Class Members provided Private Information to Defendant—either directly or through healthcare providers and their business associates—which Defendant was under a duty to keep private and confidential.

239. Plaintiff's and Class Members' Private Information is personal property, and was conveyed to Defendant for the certain purpose of keeping the information private and confidential.

240. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

241. Once Defendant accepted Plaintiff's and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendant.

242. Defendant did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

243. Defendant's failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

244. As a result of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT V
Breach of Fiduciary Duty

(On Behalf of Plaintiff and the Class)

245. Plaintiff re-alleges and incorporates by reference the above paragraphs numbered 1 to 170 as if fully set forth herein.

246. In light of the special relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information Defendant stores (and where).

247. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with patients (or the patients of their healthcare clients), in particular, to keep secure their Private Information.

248. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

249. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

250. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing

and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

251. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class Action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages,

nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Date: March 6, 2024

Respectfully Submitted,

/s/ Hart L. Robinovitch

Hart L. Robinovitch
hart.robinovitch@zimmreed.com
ZIMMERMAN REED LLP
14648 North Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400

Brian C. Gudmundson (*pro hac vice* forthcoming)
brian.gudmundson@zimmreed.com
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844

Kim D. Stephens, P.S. (*pro hac vice* forthcoming)
Cecily C. Jordan (*pro hac vice* forthcoming)
kstephens@tousley.com
cjordan@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992

Counsel for Plaintiff and the Proposed Class